S1 : Security and Privacy of Information

1. แนวทางการดำเนินงานด้าน Security and Privacy of Information ของโรงพยาบาลสตูล

โรงพยาบาลมีมาตรการคุ้มครองป้องกันด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่มีข้อมูลส่วนบุคคลของบุคลากรหรือผู้ป่วย ในด้านต่างๆ ดังนี้

1. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security)

1.1 ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ ตามความจำเป็นต่อการใช้งาน

1.2 บุคลากรที่เข้าใหม่ และต้องการเข้าใช้งานโปรแกรมต่างๆ ของโรงพยาบาล จะต้องกรอกรายละเอียดในแบบฟอร์มขออนุญาตเข้าใช้งานเป็นลายลักษณ์อักษรที่กลุ่มงานสารสนเทศทางการแพทย์

1.3 ผู้ดูแลระบบ จะทำการกำหนดสิทธิการเข้าถึงข้อมูล ของผู้ใช้งานตามหน้าที่ และความรับผิดชอบในการปฏิบัติงาน เช่น อ่านอย่างเดียว สร้างข้อมูล แก้ไข เป็นต้น

2. ความมั่นคงปลอดภัยของผู้ใช้งาน (User Security)

2.1 ผู้ดูแลระบบ กำหนดการลงทะเบียนผู้ใช้งานใหม่ ดังนี้

- จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบทำการตรวจสอบบัญชีของผู้ใช้งาน เพื่อไม่ให้เกิดการลงทะเบียนซ้ำซ้อน
- ผู้ดูแลระบบทำการเพิ่ม ข้อมูลของผู้ขอเข้าใช้งาน พร้อมทั้งจำกัดสิทธิการเข้าใช้งานให้สอดคล้องกับหน้าที่ความรับผิดชอบ
- ทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอปีละ 1 ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ยกเลิกสิทธิการใช้งาน เมื่อมีบุคลากรลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.2 การใช้งานรหัสผ่าน สำหรับผู้ใช้งาน มีดังนี้

- ผู้ใช้งานต้องรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น และไม่ควรบอกรหัสผ่าน (Password) ให้ผู้อื่นทราบ

3. ความมั่นคงปลอดภัยของระบบเครือข่าย (Network Security)

3.1 มีการแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

3.2 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารระดับสูง หรือหัวหน้ากลุ่มงานสารสนเทศทางการแพทย์ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่นๆ

3.3 ห้ามทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

3.4 ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ โดยจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น และต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

3.5 ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

4. ความมั่นคงปลอดภัยของระบบสารสนเทศ (System Security) และความมั่นคงปลอดภัยของข้อมูล (data Security)

4.1 ห้ามไม่ให้หน่วยงานที่ให้บริการผู้ป่วย ใช้โปรแกรมอินเตอร์เน็ตร่วมกับ HosXP

4.2 ห้ามไม่ให้ดาวน์โหลดไฟล์ขนาดใหญ่ที่ไม่เกี่ยวข้องกับงานในช่วงเวลา 08.00 – 16.00 น.

4.3 ห้ามปรับแก้ระบบเครือข่าย (แก้ IP และใส่ IP) จากผู้ใช้เองโดยเด็ดขาด

4.4 มีการสแกนไวรัสทุกครั้งก่อนนำอุปกรณ์บันทึกข้อมูล รวมถึงเครื่องคอมพิวเตอร์ส่วนตัวก่อนนำมาต่อพ่วงอุปกรณ์ของโรงพยาบาล

4.5 การใช้รหัสของบุคคลอื่น ในการเข้าถึงระบบเครือข่ายและข้อมูลโดยไม่ได้รับอนุญาตถือเป็นความผิดตาม พรบ. ข้อมูลข่าวสาร

4.6 ห้ามบุคคลภายนอกใช้เครื่องคอมพิวเตอร์ และวัสดุอุปกรณ์ของโรงพยาบาล

2. Monitoring (วิธีการติดตาม)

- มีการกำหนดเป็นนโยบายและระเบียบปฏิบัติอย่างชัดเจน
- จำนวนอุบัติการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และความเป็นส่วนตัวของข้อมูลสารสนเทศที่เกิดขึ้นในโรงพยาบาล < ร้อยละ 5

3. การฝึกอบรมที่เกิดขึ้น

- ประชุมและชี้แจงทำความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ความเป็นส่วนตัว และ ข้อมูลส่วนบุคคล ให้กับบุคลากรโรงพยาบาลสตูล